Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2010 Proceedings

International Conference on Information Systems (ICIS)

2010

PRIVACY ASSURANCE AND NETWORK EFFECTS IN THE ADOPTION OF LOCATION-BASED SERVICES: AN IPHONE EXPERIMENT

Mark Jeffrey Keith
West Texas A&M University, mkeith@wtamu.edu

Jeffrey S. Babb Jr.
West Texas A&M University, jbabb@wtamu.edu

Christopher Paul Furner
West Texas A&M University, cfurner@wtamu.edu

Amjad Abdullat
West Texas A&M University, aabdullat@wtamu.edu

PRIVACY ASSURANCE AND NETWORK EFFECTS IN THE ADOPTION OF LOCATION-BASED SERVICES: AN IPHONE EXPERIMENT

Completed Research Paper

Mark Jeffrey Keith
West Texas A&M University
Canyon, TX, USA
mkeith@wtamu.edu

Jeffrey S. Babb Jr.
West Texas A&M University
Canyon, TX, USA
jbabb@wtamu.edu

Christopher Paul Furner
West Texas A&M University
Canyon, TX, USA
cfurner@wtamu.edu

Amjad Abdullat
West Texas A&M University
Canyon, TX, USA
aabdullat@wtamu.edu

Abstract

The use of geospatially aware mobile devices and applications is increasing, along with the potential for the unethical use of personal location information. For example, iPhone "apps" often ask users if they can collect location data in order to make the program more useful. The purpose of this research is to empirically examine the significance of this new and increasingly relevant privacy dimension. Through a simulation experiment, we examine how the assurance of location information privacy (as well as mobile app quality and network size) influences users' perceptions of location privacy risk and the utility associated with the app which, in turn, affects their adoption intentions and willingness-to-pay for the app. The results indicate that location privacy assurance is of great concern and that assurance is particularly important when the app's network size is low or if its quality cannot be verified.

Keywords: Information privacy, mobile commerce, location-based services, network effects

Introduction

The use of mobile devices for electronic commerce (known as "m-commerce") is increasing (Kincaid 2010) as mobile broadband capabilities and devices evolve. The use of smart phones (cell phones with advanced capabilities for Internet browsing and personal productivity) has reached nearly 20 percent of all cell phone users in the U.S. (AdMob 2010). In fact, 32 percent of all cell phone users use their device to access the Internet (Rainie 2010). Some predict that over two thirds of U.S. residents will carry a smart phone by 2015 (Brandon 2010).

As Internet-enabled mobile devices gain greater market penetration, the potential for m-commerce increases – and with it the potential for new privacy and security threats. This research is concerned with one of these salient new threats in particular – the potential for mobile application (app) providers to use the location data of their users in a way that harms the user. Presently, this mobile device location data is facilitated by GPS receivers embedded into IMT-2000/3G devices, or by triangulating on radio towers. For example, Apple's iPhone allows users to purchase and download thousands of different applications. Many of these applications require the use of the device owner's location in order to make certain features more useful. One example – *Urbanspoon* – will tell its users which restaurants are closest to their position and even provide a map to the business from the user's current location. As soon as the iPhone user opens the app, it stats, "Urbanspoon would like to user your current location." If the user clicks "OK," then Urbanspoon records their current location. While this increases the utility of the app, it also begs the question: what happens to my location information?

The unintended consequences for giving this information to mobile app providers are substantial. Consider a typical traffic monitoring app which gives its users current traffic congestion updates based on their location. Because the latest iPhones have both accelerometer technology and GPS technology which can determine the physical speed at which the device is moving, these app providers could potentially sell your speed and location data to insurance providers or to the local Department of Motor Vehicles in order to determine where to place new speed cameras. Or, if you frequently search for movie rentals while at work, the app provider could use your location data to begin mailing junk mail advertisements addressed to you at your work location. Clearly, there is a need for privacy assurance of location data in mobile apps. But it is not yet understood how strong this need is in the minds of mobile app users or how substantial a role it will play on their intentions to pay for, download, and use mobile applications. We believe that the new features of these mobile devices add a new facet to the issue of information privacy which warrants further examination of personal information privacy management.

Additionally, many of these new mobile apps are heavily dependent on network effects, or the size of the base of app users (Katz et al. 1985). For example, the popular file sharing app *Bump* requires that other users have the same app installed in order to share files. An app's network size also can determine the opportunity users will have to get help from prior users of the app and help to reduce the perceived privacy risk among potential users similar to the effect that product reviews have demonstrated in electronic commerce (EC) (Duan et al. 2009).

As a result, the purpose of this research is to answer the following questions: 1) How does privacy assurance, network size, and quality influence mobile device users' intentions to adopt mobile apps? and 2) How do users make tradeoffs between these risks and rewards in determining their adoption intentions? We answer these questions using a *privacy calculus* lens (Culnan et al. 1999; Laufer et al. 1977) where the decision to adopt location-based mobile apps is based on a calculated tradeoff between the risks of giving up location data and the expected utility of the app. We integrate this with theory on network effects (Katz et al. 1985) by characterizing the utility of an app in terms of the value derived from both the non-network-based app features and the size of the network base of users. In this paper, we report the results of an experiment designed to see how manipulating three antecedents (quality ratings, privacy assurance, and network size) of users' perceptions of the risk and benefits associated with a particular app can affect their adoption intentions and willingness to pay for the app.

In the next section, we further conceptualize location privacy. Next, build our theoretical model, and outline our specific hypotheses. Following that, we describe the methodology of our simulation experiment and define our measures. After reviewing the results of the study, we discuss the findings, implications for research and practice, then outline our limitations and identify directions for future research.

Location Privacy

Information privacy has been defined as "…the ability of the individual to personally control information about one's self" (Stone et al. 1983) and "…the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent" (Haag et al. 2009, p. 227). Samuelson (2008) identified four types of privacy: location privacy, electronic communication privacy, individual information privacy and public places privacy. In this paper we are concerned with the former – location privacy – the right to limit the extent that information regarding your current and past location is recorded and shared with other parties. These concerns are not new, but recent innovations in what is becoming referred to as *location-based services* (LBS) (Bellavista et al. 2008; Xu et al. 2009) offered by geospatially-aware mobile devices and apps are bringing this issue to bear in new and compelling ways. While awareness of the effects that our technologies have on our inidividual rights to privacy have been long discussed in our literature (Mason 1986; Straub et al. 1990), it is unclear if inidivuals' perceptions and societal responses are accutely attuned to the new and evolving dimension that location privacy presents and how difficult it will be to affect those perceptions.

Recent surveys indicate that consumer electronic privacy awareness is growing (GovTech 2009). Also, many users of LBS are likely reasonably aware that there are privacy risks. However, most consumers do not understand how location data can potentially be tracked or used against them. For example, when an app requests access to the user's current location, will the app also identify them personally and tie that information to their location data? If so, the risks may be exponentially compounded. In this case, the user is not simply an anonymous person with a known location. Rather, it is John A. Doe, phone number 123-4567, email john@doe.com, located at position x. However, the multiplied risk of this information may be lost on many users.

In this sense, as most of us do in our daily lives, many consumers are taking calculated risks with the use of their private data; many assume this is a factor in the cost of realizing the utility of LBS. In this sense, this issue is typically framed as a paradox, or tradeoff weighed, between privacy and convenience (Awad et al. 2006). Essentially, the quality (and thus utility) of an information service, as would be provided by LBS, is dependent on the service provider's ability to obtain personal information from its users. The paradoxical nature of this dilemma has been studied in online, e-commerce, and other business settings (Awad et al. 2006; Culnan 1993; Ramnath et al. 2005), which has informed our inquiry into the dynamics of this problem in the mobile space. Whereas information privacy in the realm of health and financial records has clearly benefited from recent legislative imperatives (Angst et al. 2009; Damianides 2004), and while laws (both in the EU and US) are fairly specific and explicit on matters of personal information privacy ownership (Samuelson 2003), we believe individual and societal awareness has not fully subsumed the implications of geo-spatial privacy brought about by the increasing ubiquity of LBS.

While the frontier of personal information privacy had previously been crossed when computer and internet users first began to offer their financial and other personal information in the interests and pursuit of e-Commerce (Malhotra et al. 2004), the question is raised whether the use of LBS is a new increment of the same problem of personal information ownership and privacy; or, are these phenomena harbingers of new concepts and threats? To answer this question, the nature of location data must be understood and the question of ownership of this data should be discussed. Location data are those which identify the geographic location of phenomena present and locatable on the earth. The importance of the term lies in the implicit analysis, data mining, and inquiry made possible by tying information to place and space. We are interested in spatial analysis as many problem domains are concerned with relationships among phenomena situated in place (DeSmith et al. 2007).

A further privacy concern inherent in LBS lies with the "always on" nature of these devices (Sheng et al. 2008). Regardless of operating system-level controls, privacy assurance pledges and assurances and end-user vigilance, the presence of LBS are a vector for abuse and compromise of personal information privacy (Seriot 2010). For example, specifically in the case of the iPhone, the threat vectors which pose both a security threat and a privacy threat are palpable. While the iPhone API for application development is based on sound principles, the growing trend for iPhone users to "jailbreak" their devices in order to achieve greater utility also increases the risk that the device will be compromised. Furthermore, data misuse and application compromise and misbehavior are on the rise since the introduction of the iPhone in 2007 (Seriot 2010).

What is troubling about LBS, like the iPhone and applications for the device, is the relative ease with which personal information, resident in the device's "always on" flash memory, is available to application developers. Beyond just trusting an application provider via the Apple App Store, the end-user must also be concerned with what applications they don't trust with personal data might be doing. A plethora of data is obtainable by the motivated

malware developer: Google searches, YouTube history, keyboard keystroke cache, phone numbers, names, email addresses and geographic location. Each of these is exploitable, given the openly accessible and available tools inherent to the Cocoa Touch API. Moreover, despite vigilant oversight via Apple's application acceptance and screening process, it is possible to get malware into Apple's App Store (Seriot 2010).

Fundamentally, the issue we highlight with LBS is one where the overt interaction with the app is diminished and one in which the data is collected in a seamless and unnoticeable fashion (Saadi et al. 2005). In an effort to understand the implications of the incremental step represented by the availability of location data in mobile computing, it may be useful to consider the "invisible computer" phenomenon as it relates to privacy issues (See Table 1, adapted from Saadi et al. (2005)).

Table 1: The Role of GAMODAs in Invisible Computing

Invisible Computing Characteristic	General Description in Saadi et. al	Concern for Geospatial Privacy and Mobile Computing
1. Proliferation of "Smart" environments	Unprecedented and pervasive in homes, offices, cars, devices, schools, health care and elderly care	GAMODAs broadcast and otherwise communicates its presence (or is sensed)
2. Data collection is invisible	No more card swiping or form signing, as sensors in walls, doors, and shirts silently collect information	GAMODAs exhibit agency on behalf of its owner/user – transacting on the owner's behalf without intervention
3. Data intimacy	Not only what we do, where we do it, and when we do it, but also how we feel while doing so (as expressed by our heart rate, perspiration, or walking pattern)	The attraction of GAMODAs lies in the information convergence and synergy they facilitate. Users are empowered by the convenience of the device. Privacy is harder to maintain when unrelated concerns converge into a single device.
4. Data Voracity	Smart objects are dependent on as much information as they can possibly collect in order to best serve us.	GAMODA utility increases as wider and interrelated datasets are introduced and used
5. Data Cooperation	The increasing interconnectivity allowing smart devices to cooperatively help us means an unprecedented level of data sharing; making unwanted information flows much more likely	Typical GAMODA use patterns involve cooperatively sharing data seamlessly among apps (and, accordingly, across app providers)

The implication of Table 1 is that LBS are poised and able to provide the interactions described in the "invisible computer" environment. When considered in this context, the tradeoff between privacy implications and convenience/benefit implications of geospatially-aware mobile device use becomes clearer. As has been the case with the diffusion of so many other innovations, the early-adopters likely possess both the socio-economic, intellectual and contextual capacity to make an informed decision on the transaction costs involved when using LBS (Rogers 2003). However, much as was the case with PC adoption and Internet adoption, as the adoption rate for LBS increases, it is likely that the location privacy problems will be more acutely felt. As increased LBS use contributes to ubiquitous, relentless and constant "invisible computing" data collection, the effects of location data in the mix of privacy concerns will be easier to detect using empirical means.

Theoretical Foundations

Privacy Calculus

Although research on the adoption of LBS and mobile apps in particular is still relatively young, theory on privacy calculus is emerging as an appropriate lens for its examination (Culnan 1993; Culnan et al. 1999; Dinev et al. 2006; Xu et al. 2008; Xu et al. 2009). Privacy calculus draws from prior theories typically used to study the adoption of IT such as the *theory of reasoned action* (TRA) (Ajzen et al. 1980), the *theory of planned behavior* (TPB) (Ajzen 1991), and the *technology acceptance model* (TAM) (Davis 1989). In particular, it is based on the same notion that

perceptions and beliefs regarding IT lead to behavioral intentions (Dinev et al. 2006). This approach is similar to McKnight et al.'s (2002) theoretical model of trust in electronic commerce (EC) and Gefen et al.'s (2003) theoretical integration of trust and TAM. Privacy calculus refers to the beliefs which lead to a user's intention to provide personal information in order to transact with an IT. In the present context we are concerned with the beliefs which lead a user to disclose their location data in order to realize the utility of LBS, and in particular, mobile apps. However, unlike TRA, TPB, and TAM, privacy calculus supports the notion that the behavioral intentions can be influenced by *contrary* beliefs. In other words, the decision to use a mobile app or other LBS is based not only on the benefits such as usefulness and ease of use, but the risks associated with disclosing location data. As a result, the user makes a calculated decision in which the risks are traded for the benefits.

We believe that privacy calculus is especially applicable to the LBS context and mobile apps in particular. As the number of available apps for iPhone and Android users rises into the hundreds of thousands and with iPhone users downloading about two new apps per month (Gigaom 2010), mobile apps present many opportunities for users to make the risk-benefit tradeoff decision. Yet the research on privacy calculus decisions regarding LBS is still relatively sparse. One notable exception (Xu et al. 2009) integrates a privacy calculus model with *justice theory* (Colquitt et al. 2001) to understand how the fairness perceptions of a firm's information privacy practices affects users' decisions. Xu et al. (2009) focused on two dimensions from justice theory: 1) procedural justice, which refers to the perceived fairness of the procedures used to collect information, and 2) distributive justice, which refers to the perceived fairness of the outcomes from sharing personal information. They discovered that compensation (in the form of monetary rewards), institutional privacy assurances, and governmental privacy regulations can influence a user's perceptions regarding the risks and benefits of using LBS.

To advance this line of research, we incorporate theory on network effects (Katz et al. 1985) to demonstrate how privacy assurance is calculated against the benefits of network size and LBS quality to influence a user's behavioral intentions to disclose their location information. Figure 1 visualizes the two theoretical lenses.

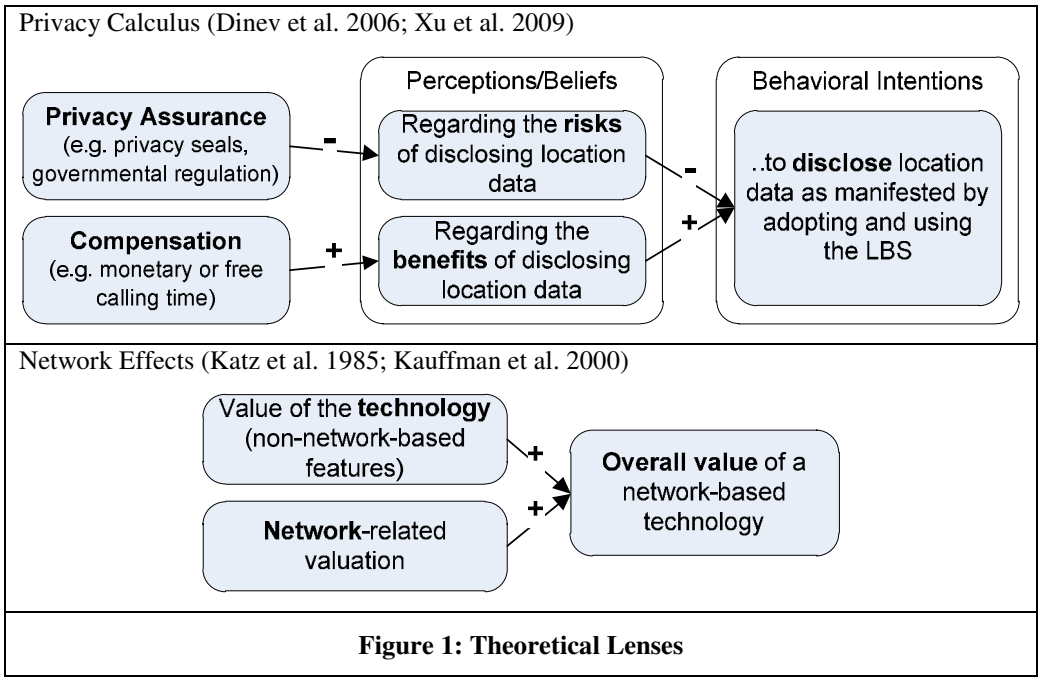

Figure 1: Theoretical Lenses

Network Effects

Network effects, or externalities, refer to the positive or negative value associated with an increase in the number of agents consuming a particular good or service (Katz et al. 1985). It has been demonstrated that the value of an IT, and its subsequent adoption, depends on both the value placed by the consumer on the non-network-based features of the technology itself as well as the value of the network base (Kauffman et al. 2000). For example, consider the mobile app *MouseWait* which gives its users real-time updates about the current wait times for each of the rides at the *Disneyland* theme park. The source of the current wait times comes from current users recording their start and

stop times while waiting in lines. If there are only a few users, then the information produced by the app is likely to be less accurate. But as more people use the app, the wait times become increasingly accurate. Based on this theory, we argue that if privacy calculus holds, and users take into consideration all of the benefits of disclosing their location data, that their perceptions will be influenced by both the value of the app technology as well as the size of its network base of users. The value of the app technology refers to the consumer's valuation of its non-network impacts (Kauffman et al. 2000). In the MouseWait example, this would refer to the other information it offers such as maps of the park, hours, and other less dynamic information. This would also refer to the technical quality of the app itself and the quality of the user interface.

The overall value of a network-based mobile app can also be framed as a type of distributive justice as outlined in justice theory. Essentially, the user is trading their location data in return for access to the information provided by having a large network base of users (Colquitt et al. 2001). Therefore, they perceive fairness in the outcome and a greater benefit of disclosing their location data. Based on the discussion above, we believe that the perceived benefits of disclosing personal information is better explained by network theory in the mobile app context than from compensation in the form of money or free calling time (c.f. Xu et al. 2009).

Hypotheses Development

To be clear, the core of our theoretical model is based on privacy calculus where the intention to disclose location data is based on a calculated tradeoff between the associated risks and benefits. However, based on the above discussion we also integrate from theory on network effects to frame the antecedents of the risk-benefit perceptions in addition to privacy assurance. Our research model is illustrated in Figure 2.

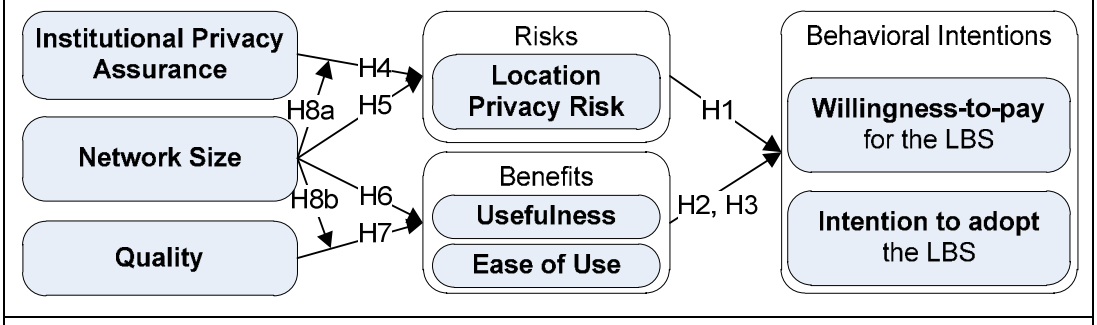

Figure 2: Research Model

As dependent variables, we use both intention to adopt LBS (INT) and willingness-to-pay for LBS (WTP). INT is taken from the TAM literature (Davis 1989) and represents the users behavioral intentions to fully appropriate the LBS and, by doing so, disclose their location data. WTP, on the other hand, is an economic variable which provides greater insight into the level of adoption intention. The mean of WTP would traditionally be a measure of the potential value of the LBS, or, the consumer's maximized utility subject to budget constraints. WTP is relatively less-frequently used in IT research and even marketing research in general despite the fact that price is a key element in the adoption decision (Homburg et al. 2005). It has also been recently used in studies of network effects to represent the value of a network-based technology (Raghu et al. 2009).

Perceived Benefits Regarding LBS

The unique benefit of using LBS is the ability to use the positioning features in order to provide a more personalized experience and information (Xu et al. 2009). However, this is only one of several benefits derived from these mobile apps. Therefore, we draw from TAM and trust theory to employ the more general measures of perceived usefulness (PUSE) and perceived ease of use (PEOU). These variables have been used in a variety of studies and theories on EC and mobile technology adoption (Gefen et al. 2003; Vance et al. 2008) and have been demonstrated to positively influence adoption intentions (Davis 1989; Venkatesh et al. 2003).

PUSE is "a measure of the individual's subjective assessment of the utility offered by the new IT in a specific…context" (Gefen et al. 2003, p. 54). It reflects the ability of an IT to help users be more productive and efficient in their work and improve their performance. In the case of LBS, this means that being able to customize the information to the user's location helps them accomplish tasks more quickly and/or perform at a higher level. Consider the popular app *RedLaser* which allows users to take pictures of the bar codes on any product and receive an immediate list of local retailers who offer that product sorted by lowest price with a map to each location. If the user is willing to provide RedLaser with their current location, this reduces search costs and lowers their total transaction costs. Certainly, this benefit of disclosing location data would help the user be more productive and efficient. Similarly, greater PUSE of a mobile app reflects greater utility and value.

PEOU is a measure of the cognitive effort required how to learn to use a new IT. Lower learning costs result in being able to fully utilize a new IT more quickly. Research has demonstrated that if users act rationally, as predicted in TRA, they will be more inclined to use new IT with greater PEOU (Venkatesh et al. 2003). Therefore:

H1: PUSE will positively affect INT and WTP for LBS.
H2: PEOU will positively affect INT and WTP for LBS.

Perceived Risks Regarding LBS

Perceived risk has a variety of dimensions including privacy risk (Malhotra et al. 2004). Perceived privacy risk refers to the user's belief that the degree to which they disclose their personal information will lead to an associated loss (Featherman et al. 2003). Privacy risk is typically operationalized as a single dimensional construct measuring the loss of control specifically over personal information (Xu et al. 2009). We use the single dimensional construct *location privacy risk* because we are interested specifically in effects of losing location data.

Research has demonstrated that perceived privacy risk has a negative impact on a user's behavioral intentions to disclose personal information through EC transactions (Dinev et al. 2006; Malhotra et al. 2004). In the LBS context, opportunistic behaviors regarding location data – particularly matching the location data to a person's identity – can result in unwanted solicitations, more personalized spam email and junk mail, or even personal embarrassment (Clarke 2001). Therefore, we make the following hypothesis:

H3: Perceived location privacy risk will negatively affect INT and WTP for LBS.

Antecedents of Perceived Benefits and Risks

Privacy Assurance

Privacy assurance refers to the interventions taken by LBS providers to assure users that steps have been taken to protect their personal information (Xu et al. 2008). This relationship is also supported by theory on trust in EC (Gefen et al. 2003; McKnight et al. 2002). Privacy assurance is similar to (and based on) the concept of *structural assurance* which refers to the use of privacy seals, guarantees, and promises found in EC transactions which positively influence trusting beliefs. Institutional privacy assurances have been demonstrated to significantly increase trust and reduce perceived risks in mobile EC context (Vance et al. 2008; Xu et al. 2009). Therefore:

H4: Institutional privacy assurance will negatively affect perceived location privacy risk for LBS.

Network Effects

As discussed above, network effects shed light on the overall value, or benefit, of LBS such as mobile apps. Research has demonstrated that the overall value of an IT is derived from both the non-network-based benefits (e.g. system quality, information quality, etc.) as well as the network size (Katz et al. 1985; Kauffman et al. 2000). We argue that network size can influence both the perceived benefits and risks of disclosing location data.

First, we refer to the *primary* benefits of network size which are inherent in *some* LBS. For example, the MouseWait app described above becomes increasingly accurate, and therefore useful, as the number of users increases. These direct benefits should affect PUSE. There are also *secondary* benefits of network size which can be realized by *all* LBS. For example, the restaurant information made available in the Urbanspoon app described above is produced by the app provider and not its users. But the user interface for Urbanspoon is quite unique, albeit interesting. Even though it may seem intuitive to some users, there may be less-technically savvy users who would benefit from

having a friend or family member teach them how to use it. As more consumers adopt Urbanspoon, there is a greater likelihood that future users will be able to get help learning to use the app from among their immediate social network connections, making the app seem like it will be easier to use. Essentially, network size can reduce users' perceived learning costs which have been demonstrated to play an important role in the overall transaction costs of a product or service (Farrell et al. 2007).

Network size can also play a role in reducing the information asymmetry which raises the uncertainty costs associated with a transaction (Williamson 1981). As the network size increases, future potential users may perceive the prior adopters as assurance that the LBS provider will not behave opportunistically with their location data, that the LBS will be easy enough to learn, and that the LBS is sufficiently useful. In summary:

H5: Network size will negatively affect the perceived location privacy risk associated with LBS.
H6: Network size will positively affect the PUSE and PEOU of LBS.

Quality

As stated above, the overall value of an IT is based on both the network-dependent value as well as on non-network-dependent value (Kauffman et al. 2000). In other words, in addition to the network size, system quality and information quality will also determine the overall value and benefit of LBS. The *quality* construct is well-established in theory on IT success (DeLone et al. 2003) and has been used extensively in EC research to refer to characteristics of a website such as the presence of bugs, the ease of the user interface, and navigational structure (McKnight et al. 2002; Seddon 1997; Vance et al. 2008). As with these prior studies, we hypothesize:

H7: Quality will positively affect the PUSE and PEOU of LBS.

Interaction Effects

In addition to the direct effects hypothesized above, we also believe that there are likely to be significant interaction effects among the institutional privacy assurance, network size, and quality of LBS and mobile apps in particular. Contemporary *choice theory* posits that users' choices are made in order maximize their utility which is based on a decomposable set of contributors or attributes which can be economic or psychological (Hui et al. 2007; McFadden 1986). Hui et al (2007) explains that people make tradeoffs among these attributes so that the disutility due to undesirable attributes is compensated by the utility of desirable attributes. In the present context, institutional privacy assurance, quality, and network size are all attributes of the user's choice. Because consumers make tradeoffs among the attributes of a product in order to maximize their utility (or minimize perceived risk), they may be willing to accept lower quality if the network size is sufficiently large. Or, they may worry less about the absence of institutional privacy assurances if many other people appear to trust the app. Therefore:

H8a: Large (small) network size will reduce (increase) the effect of institutional privacy assurance on the perceived location privacy risk associated with LBS.
H8b: Large (small) network size will reduce (increase) the effect of quality on PUSE and PEOU of LBS.

Research Methodology

To test our hypotheses, we selected Apple iPhone apps as the LBS of interest. The iPhone is currently growing faster than the industry leader, Blackberry, yet it still comes in a distant second in overall market share to Blackberry devices which have been available for several more years (AdMob 2010; Kincaid 2010). This means first time adoption of the iPhone platform is still taking place at a very high rate relative to its competitors. This is important because trust and privacy issues are a top concern when users adopt an IT or EC channel which they're unfamiliar with (Gefen 2000; Gefen et al. 2003; McKnight et al. 2002; Vance et al. 2008). To test the hypotheses, we used a 2 x 2 x 3 factorial experimental design for a total of 12 different groups. The treatments were privacy assurance (none versus low versus high), quality rating (low versus high), and network size (small versus large). Table 2 summarizes the number of individuals in each group.

Table 2: Experimental Design					
		Low Quality		**High Quality**	
		Network Size			
		Small	Large	Small	Large
Institutional Privacy Assurance	None	45	45	46	45
	Low	46	45	46	46
	High	46	45	46	46

Based on a pilot test of 26 participants, four different iPhone app contexts were selected from the iPhone App Store for the experiment which reflected a variety of the salient uses of mobile apps which incorporate location data: 1) an app which gave real-time updates on traffic congestion along commonly used roads and highways, 2) an app which allowed its user to map their fitness routes for running, biking, etc. and recorded their times, 3) an app which located friends and family members on a map, and 4) an app which mapped and located registered sex offenders in the user's area. These apps are not meant to represent variations in the independent variables, but rather to offer a range of contexts in order to reduce the variance attributed to any un-captured context-dependent variables. However, two of them (the fitness and locator apps) were specifically chosen because they offer a direct network-based value to their users. Users of App 2 can upload their favorite fitness routes so that they can be shared with others and App 3 will only locate friends and family members using the same app. App 1 and 4 still offer indirect network-based value in that as more people adopt those apps, the uncertainty and potential learning curves of future users will be increasingly reduced.

Measures

Institutional Privacy Assurance, Network Size, and Quality

Quality, institutional privacy assurance, and network size were each measured in two ways. First, they were manipulated in the experimental design. Quality is manipulated by using Adobe Photoshop to make one version of the app with one out of five stars (low quality) and another version with five out of five stars (high quality). The stars represent an overall rating reported by prior users. Network size was manipulated by editing the number of total reviews. Small network sizes for the four contexts received less than 10 reviews whereas large network sizes received over 10,000 reviews. Privacy was manipulated in the description by including either no mention of privacy assurance (no assurance), a Better Business Bureau (BBB) privacy seal only (low assurance), or a BBB seal, VeriSign seal, and written "Privacy Promise" (high assurance). Second, we captured their perceptions of quality (McKnight et al. 2002; Vance et al. 2008) and network size (Burnham et al. 2003; Keith et al. 2010) using Likert-type items (1=strongly disagree; 7=strongly agree) drawn from validated instruments. We then used these perceptual measures as checks to see if our manipulations for quality and network size were valid by comparing the mean of the measurement items for each variable between groups. Participants perceived the large network sizes (M = 5.07) as larger than the small network sizes (M = 3.76), one-way ANOVA, F = 24.27, $p < 0.001$. They perceived the higher quality-rated apps (M = 5.53) as higher than the low quality-rated apps (M = 4.84), one-way ANOVA, F = 7.44, $p = 0.008$. The measure for perceived location privacy risk (described below) was used as a validation check for our manipulation of institutional privacy assurance and it appears valid. Participants perceived the high privacy assurance (M = 4.41) as greater than the low privacy assurance (M = 3.90) and the low privacy assurance greater than no privacy assurance (M = 3.83), one-way ANOVA, F = 19.32, $p < 0.001$ (contrasts between group pairs were both significant at $p < 0.001$, indicating that our manipulations were successful).

Figure 3d demonstrates the manipulation in the description screenshot from one of the four apps used in the experiment.

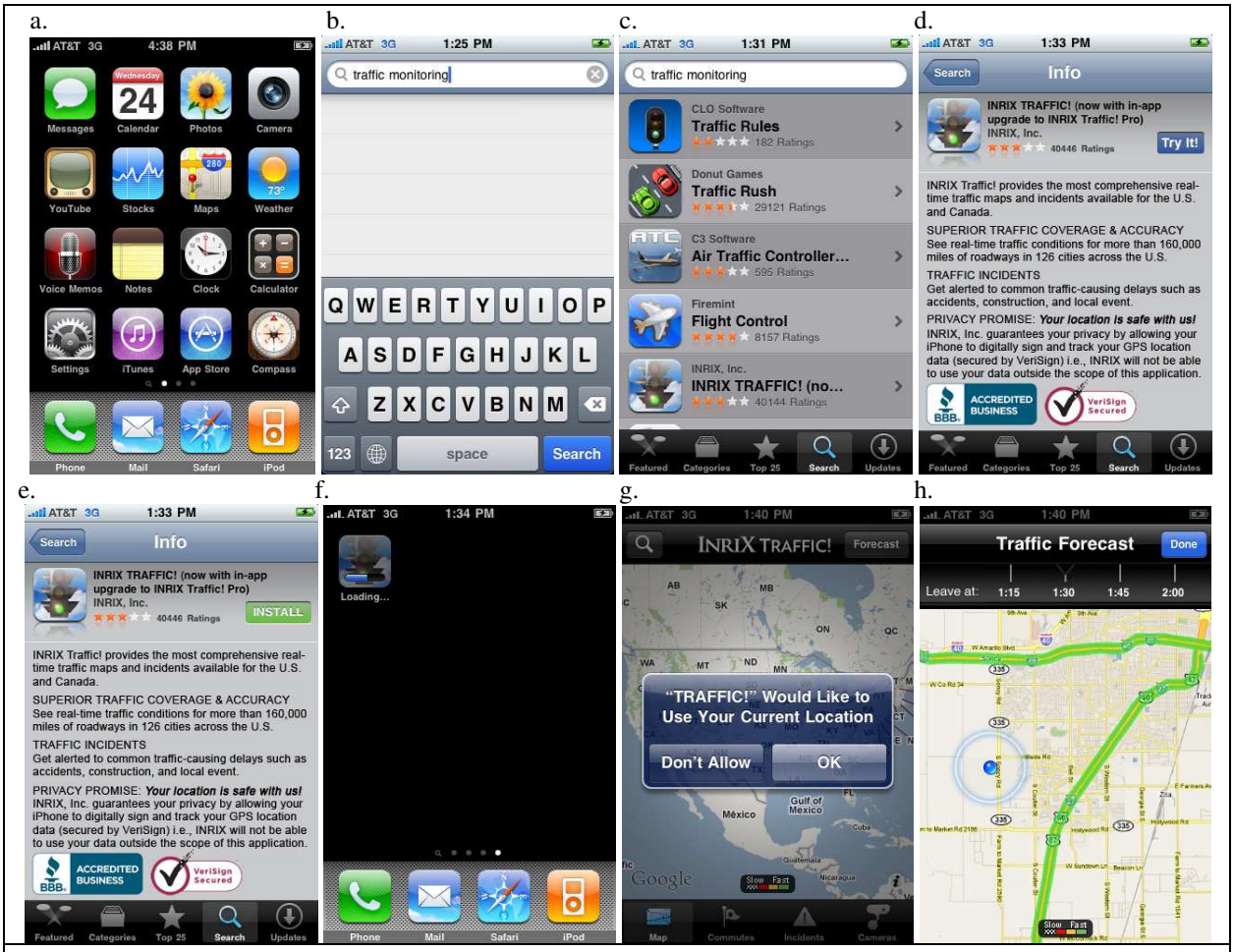

Figure 3: Simulation Example (eight of the ten screen shots in total)

Perceived Risks, Benefits, and Behavioral Intentions

Perceived location privacy risk was measured with items created similar to prior research (Xu et al. 2009), but focusing primarily on *location* privacy. In particular, they addressed whether the participant believed the app provider would share, sell, or otherwise use their location information unethically. The four privacy items were developed by: 1) reviewing privacy dimensions in existing research (Seriot 2010; Smith et al. 1996; Xu et al. 2009), 2) pilot testing the items (n=26), 3) interviewing the pilot participants for feedback, and 4) validating them using techniques for reflective constructs ($\alpha = 0.92$; see statistics below).

PUSE, PEOU, INT were all based upon well-validated instruments from existing TAM research (Davis 1989; Venkatesh et al. 2003) with minor changes to reflect the four contexts of use described above.

While WTP is not a perception-based item like adoption intentions, it is still only a hypothetical measure of the utility participants will derive from the mobile app subject to budget constraints – not a measure of actual monetary outlay. Therefore, we used the stated-choice method which is similar to many marketing studies on WTP (Cameron et al. 1987; Homburg et al. 2005; Krishna 1991) where the participants are simply asked, "How much would you be willing to pay for [mobile app name]?"

Control Variables

Several controls were also included, many of which were found relevant in similar studies (Hui et al. 2007; Xu et al. 2009). Typical demographic variables including age and gender were measured. A control for the context of the mobile app was included as a predictor of each variable. Participants were also asked if they currently used a smart

phone or other mobile device (e.g. iPod touch or PDA) capable of downloading and installing mobile apps. They were also asked to indicate the number of transactions they had made in the last year over a mobile device (an indicator of their mobile EC experience) and how many times their personal information had been misused as the result of any EC transaction to their knowledge (and indicator of the privacy risk experience).

During the experimental procedures, two-thirds of the participants received treatments which included a BBB privacy seal (for the low and high institutional privacy assurance manipulations). The web application included a link ("What does the BBB seal mean?") which allowed the participant to open a pop-up window from the actual BBB website which describes exactly what the BBB seal meant. The application recorded which users clicked on that link. Therefore, the last control variable included in our study was a true/false indicator of whether or not the participant clicked on that link to better understand the purpose of the BBB seal.

Participant Recruitment and Experimental Procedures

Because the largest demographic of mobile internet users is those ages 18-29 (Rainie 2010), student participants were recruited at two major universities. Both are large public universities in the United States – one in the Midwest and another in the Southwest. Between those universities, 1213 undergraduate and graduate students from their respective business colleges were solicited for participation in the experiment which took place outside of regular class time. They were offered both extra credit as well as a chance to win one of several $50 gift cards. Of those who were solicited, 667 agreed to participate (55 percent response rate), and 547 of those successfully completed the entire experiment. The experiment involved three steps. Each participant completed the experiment individually and took as much time as needed. Most participants spent between 15 and 25 minutes. In order, the steps involved were:

(1) Each participant navigated to the website where the experimental simulation was hosted. After reading a cover letter, they were given a pretest in order measure their disposition to trust and their attitude toward institution-based trust using the items described above (similar to Vance et al. (2008)).

(2) Next, they were randomly assigned by the web application to one of 48 different simulations (12 group manipulations x 4 contexts) so that each participant viewed a simulation of one particular context. To accomplish this, an algorithm was written which measured the current number participants in each of the 48 groups, sorted those groups by the count of completed surveys, and then randomly assigned the next user to one of the groups with the lowest count. This assured both random and equal assignment to treatments.

(3) Next, they were given one of the four hypothetical scenarios to consider. For example:
You have recently purchased a new Apple iPhone and you would like to download an application which will give you current updates about the traffic congestion during your commute to and from work. This application would be very useful to you because there are multiple routes you could potentially take each day and traffic congestion makes a big difference in how long your commute takes.

The following images are hypothetical screen shots from an iPhone which walk you through the steps required to find and download an app which will serve your purpose. Please review the screen shots in detail and take special notice of the description of the selected app and the rating it received from other customers.

(4) After checking a box to confirm that they read and understood their scenario, they were then given a series of 9-12 screen shots (depending on the context) which simulated the process of searching the Apple App Store for an app which met their needs, downloading and installing the app, opening the app, and using it once for its intended purpose. The screen shots allowed the user to use their mouse to click the actual buttons on the iPhone images in order to complete the simulation. These screen shots were based on actual images from an iPhone, but modified in order to reflect differences in privacy assurance, quality ratings, and network size (See Figure 3 above).

(5) After completing the simulation, they were given a post-test which included all of the remaining measures described above. It also included a series of manipulation checks to see if they remembered their treatment (e.g. "How many stars out of five did this app receive on average from prior users?" "How many ratings did this app receive?" "Was there a privacy statement?" "Was there a BBB seal?"). Results indicate that over 90% remembered all of their treatments which compares well to similar studies (Hui et al. 2007).

Data Analysis and Results

PLS (partial least squares, SmartPLS version 2) was used to analyze the data. Because we needed to evaluate all paths in a single analysis, structural equation modeling (SEM) analysis was chosen over regression (Gefen et al. 2000). PLS does not depend on normal distributions and interval scales (Fornell et al. 1982) making it better-suited for incorporating our WTP measure and control variables. Additionally, PLS is ideal for testing theory in the developmental stages (Fornell et al. 1982). Because our integration of network theory with privacy calculus is unique to this study, PLS was deemed appropriate. In the structural model tested, the manipulation check scores for privacy, quality, and network size were used because they reflected the participants' perceptions as affected by the treatments (similar to Komiak and Benbasat (2006)). All measurement items were standardized.

Measurement Validation

The measurement properties of the instrumentation are analyzed through reliability and convergent/discriminant validity. Convergent validity is measured by the reliability of items, composite reliability of constructs, average variance extracted (AVE) (Barclay et al. 1995; Hu et al. 2004), and factor analysis. Reliability is measured by examining each item's loading on its construct. In this study, all item loadings are well above 0.70 as suggested by Barclay et al. (1995). Composite reliability scores ranged from 0.87 to 0.97 which is well above the suggested 0.70 benchmark (Barclay et al. 1995; Fornell et al. 1981) demonstrating internal consistency. The AVE measures the amount of variance captured by a construct from its indicators compared to the amount due to measurement error (Chin 1998) and it's recommended to exceed 0.50 (Hu et al. 2004). AVE scores for each construct in this study range from 0.72 to 0.94 satisfying the condition. In order to demonstrate good convergent validity in the factor analysis results, all items should load on their own latent variables above 0.32 at a minimum, but preferably above 0.71 (Tabachnick et al. 2000). This requirement was met.

Discriminant validity is measured by examining confirmatory factor analysis (CFA) results, cross-loadings, the relationship between correlations of all constructs, and the square root of AVEs (Chin 1998; Fornell et al. 1981; Komiak et al. 2006). The CFA results (df = 1457, X^2 = 2780.24, RMSEA = 0.045, NFI = 0.96, CFI = 0.98) demonstrate strong discriminant validity because all measurement items load highly (above 0.72) on their own constructs and more so than on any other construct (Boudreau et al. 2001; Chin 1998; Gefen et al. 2000; Straub 1989). Also, according to Fornell et al. (1981), the square-root of AVEs should exceed the correlations among constructs, indicating that more variance is shared among construct indicators than with other constructs. This condition was also met for each construct indicating adequate discriminant validity.

Common Methods Variance

Harman's single-factor test was conducted to test for common methods variance (Podsakoff et al. 2003). Essentially, this test is designed to see if a single factor emerges from an exploratory factor analysis (unrotated) or if one overall factor accounts for most of the covariance among measures (Podsakoff et al. 2003, p. 889). Our unrotated component matrix yielded 11 factors and the largest factor only explained 28% of the total variance indicating a low likelihood of common methods variance.

Hypothesis Testing

Our hypotheses were tested through the PLS structural model (See Figure 4). The explanatory power of the model is assessed through the R^2 scores (i.e. the amount of variance accounted for) and the latent variable paths. In this study, we explained 39.5 percent of the intent to adopt, but only 11.3 percent of WTP. Intent to adopt was affected by location privacy risk (β = -0.23, $p < 0.001$) and PUSE (β = 0.31, $p < 0.05$), but not PEOU. WTP was affected by location privacy risk (β = -0.63, $p < 0.001$) and PUSE (β = 0.26, $p < 0.05$), but not PEOU. However, WTP was explained by the participant's age (β = 0.10, $p < 0.05$), whether or not they clicked the BBB definition link (β = 0.06, $p < 0.05$), the number of EC purchases made using a mobile device (β = -0.19, $p < 0.01$), and the extent of prior information misuse they had experienced (β = -0.17, $p < 0.05$). The context of the mobile app used in their version of the experiment, gender, and whether or not they were smart phone users were not factors in participant's WTP and are left out of the diagram for simplicity. None of the control variables significantly affected INT.

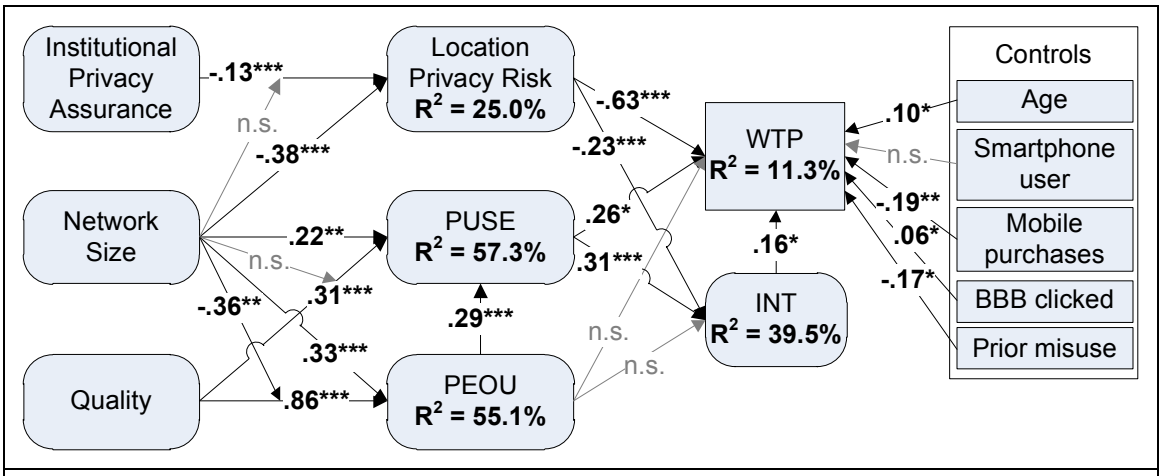

Figure 4: Results of PLS Analysis (Note: * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$)

Twenty-five percent of perceived location privacy risk, 57.3 percent of PUSE, and 55.1 percent of PEOU were explained in our model. As expected, institutional privacy assurances significantly reduced perceived location privacy risk ($\beta = -0.123$, $p < 0.001$). Also, perceived mobile app quality positively influenced PUSE ($\beta = 0.31$, $p < 0.001$) and PEOU ($\beta = 0.86$, $p < 0.001$). Network size had a large negative effect on perceived location privacy risk ($\beta = -0.38$, $p < 0.001$) and also had the expected positive effect on PUSE ($\beta = 0.22$, $p < 0.01$) and PEOU ($\beta = 0.33$, $p < 0.001$). Contrary to H8a and H8b, network size did not moderate the effect of institutional privacy assurances on perceived privacy risk or the effect of quality on PUSE. However, network size did have a negative moderation effect on the impact of quality ratings on PEOU ($\beta = -0.36$, $p < 0.01$). In other words, in the case of large network sizes, participants placed less emphasis on the quality ratings in determining their PEOU.

The effects of the mobile app context are not visualized in Figure 4 for simplicity. However, context did play a significant role in determining PUSE ($\beta = 0.27$, $p < 0.05$). Also, in a post hoc analysis, context was a significant moderator of the effect of network size on perceived location privacy risk ($\beta = 0.19$, $p < 0.01$) and network size on PUSE ($\beta = -0.09$, $p < 0.05$).

Discussion

Using a privacy calculus model integrated with theory on network effects, this study investigated the effects of institutional privacy assurance, quality, and network size on users' adoption intentions and WTP for mobile apps which employ LBS. H1 through H7 were confirmed with the exception of H2 – after accounting for the impact of perceived location privacy risk and PUSE, PEOU did not have a direct effect on WTP or adoption intentions. We also find that institutional privacy assurance mechanisms (e.g. privacy seals and stated promises) can reduce a user's perception of location privacy risk. However, what is interesting is that the coefficient for the effect of network size is almost three times larger ($\beta = -0.38$) than that of the effect of privacy seals and stated promises ($\beta = -0.13$) in reducing perceived location privacy risk. In other words, privacy fears can be better-mitigated by a large network base than privacy seals. Perhaps participants believed that, "if everyone else trusts it, then I can too;" yet the large network size does not change the importance of privacy seals and stated promises in the minds of users. Also, although network size can positively influence PUSE and PEOU, perceived app quality (as determined by the average star rating by prior users) plays a stronger role in determining PUSE ($\beta = 0.31 > \beta = 0.22$) and PEOU even more so ($\beta = 0.86 > \beta = 0.33$). In summary, while perceived privacy risk is most affected by network size, PUSE and PEOU are most affected by quality ratings. However, this is dependent upon the context of the app.

The control variables appear to affect WTP as might be expected. For example, older participants were willing to pay more for the app ($\beta = 0.10$, $p < 0.05$). Greater age likely indicates greater earning power and wealth. Also, those who had more experience with making purchases such as apps for the iPhone were willing to pay less ($\beta = -0.19$, $p < 0.01$). Apps for the iPhone typically range from free to only a few dollars. It's possible that those with more experience simply knew that they could likely get a free version or that most apps were very inexpensive. Those who had experienced more information misuse were willing to pay less for their apps ($\beta = -0.17$, $p < 0.05$), likely because they had a greater realization of the threats. And lastly, those who clicked the "what's this?" link to read

what the BBB privacy seal meant were willing to pay more for their app ($\beta = 0.06$, $p < 0.05$), perhaps because they had a better understanding of the significance of the BBB seal.

In a post-hoc analysis, several interaction effects proposed in prior IT acceptance research (Venkatesh et al. 2003) were examined to see how factors such as experience, age, gender, etc. influence the adoption intentions. In particular, the participant's level of prior information misuse ($\beta = 0.25$, $p < 0.05$) and whether or not they were a smart phone user ($\beta = -0.20$, $p < 0.05$) moderated the effect of perceived location privacy risk on WTP. Also, age moderated the effect of perceived location privacy risk on INT ($\beta = 0.62$, $p < 0.05$). Lastly, PUSE moderates the effect of perceived location privacy risk on WTP ($\beta = -0.31$, $p < 0.05$) indicating that users may be willing to trade a certain amount of location privacy risk for greater utility.

Also as part of a post-hoc analysis, we examined the direct effects of institutional privacy assurance, network size, and quality ratings directly on WTP and INT. Institutional privacy assurances significantly impacted WTP ($\beta = 0.$, $p < 0.001$) and INT ($\beta = 0.$, $p < 0.001$).

Finally, while network size does appear to serve as a surrogate for quality ratings in determining PEOU ($\beta = -0.36$, $p < 0.05$) to a certain extent, users appear to base PUSE on quality ratings and network size independently of each other. In other words, if I can see that an app has been downloaded and rated many times, than I'm less worried about whether or not the quality rating accurately reflects how easy the app is to use. However, I'm just as concerned about whether or not the quality rating accurately indicates the usefulness of the app.

Implications for Research

Broadly speaking, our research efforts should, positively impact theory and practice. In the context of personal privacy in an always-on and omnipresent information environment, this research presents a starting point in our understanding of LBS use as it pertains to location privacy. The implications this study has for theory and research center largely on this study's focus on location privacy. We find that location privacy is an emerging and important concern in m-commerce adoption models as well as privacy/security research.

Specifically, we have found that when and where location privacy risk is a concern, users will place as great of importance on their perception of the level of that risk as they do on their perceived usefulness. And, the prevailing proposal that consumers will, under certain circumstances, trade privacy assurance for convenience is confirmed by this study to an extent. In particular, we find that contemporary *choice theory* explains this phenomenon well: users want to maximize their utility from the LBS. End-users will derive utility from certain LBS attributes; thus an end-user's optimization on one attribute can be exchanged for compromise on another in order to maximize their overall utility function. This is consistent with the long-understood phenomenon of satisficing (Simon 1982), where it is likely that these choices are made with imperfect information and in the light of uncertainty because it is too costly to obtain perfect information. As LBS use increases, and thus as compromises and other attention-grabbing cases arise, it remains to be seen how deeply location privacy is affected. Will information imperfection and uncertainly continue to rule, or, will location data become among the many privacy concerns already under consideration? In essence, will LBS do for information privacy awareness what the advents such as email and the World Wide Web have done in the past?

Implications for Practice

The results of this study carry substantial implications for practice. Generally, we found that: (1) measures and mechanisms which provide privacy assurance are critical if you haven't built a network of users yet, which is the case for many mobile application developers working within the developing LBS market; (2) even within a large network, a low-rated (and thus perceived as low-quality) app must compensate with strong privacy assurance measures and mechanisms; (3) strong ratings and/or a large network may give a false sense of privacy assurance; and, (4) There is a need for "privacy assuring" measures and mechanisms. In light of number four, privacy assuring mechanisms will be realized as a multilateral effort involving users, application developers, information aggregators and disseminators, and device manufacturers. While security controls can ensure that data transmissions are encrypted, the most pressing problems exist at the terminals of a transaction: (1) with the user and the device and (2) with the retention and use of location data, once it is collected. Security and privacy assurance mechanisms have matured in areas such as medical records (Ateniese et al. 2003) and e-commerce (Duh et al. 2002), however, control mechanisms that rely on a commercially-interested party can only go so far in the long run.

It is probable that, the results of this study notwithstanding, LBS users and those interested in information privacy assurance will have to take personal responsibility for the protection of their privacy. Technical solutions which might facilitate users' personal responsibility might resemble the Certificate Authority (CA) and Public Key Infrastructure (PKI) systems in place to ensure data integrity using paid 3rd parties. As a CA typically issues a digital certificate in order to verify the identity of the owner, a similar 3rd party could verify that location data (or other such private data) has also been signed in a manner consistent with PKI. Just as CA companies such as WebTrust, Thawte, Geotrust and VeriSign have enjoyed steady growth given the ubiquity of the PKI system of security assurance using SSL, so too could a business model emerge which uses similar technology for location data oversight and audit. It would seem that as risk management industries exist to hedge against the contingencies of risk, so too could an infrastructure arise which used PKI techniques to allow consumers to purchase policies against the risk of privacy compromise. As risk underwriters are vested in preventing risk, those that submitted to such a system (users, application providers, etc.) would mutually benefit from such an arrangement. It is likely that an artifact/prototype demonstrating such an infrastructure would be a logical response to the outcomes of this research and it is indeed among our planned future research efforts on this matter.

Limitations

As with any study which undertakes to sample from a growing and unsettled population, this study is not without limitations. Given the emergent nature of LBS and the nascent concern for location privacy, we share the following concerns regarding this study.

With respect to our experimental design and the generalizability of our results, we acknowledge that ours was not a truly a random sample. However, all participants were solicited based on their being valid and likely consumers/users of mobile applications. Additionally, 61 percent of participants reported to have been currently using devices capable of purchasing and using mobile applications. Thus, we are confident that our convenience sample is drawn appropriately in order to generalize to the appropriate and desired context.

Another concern lies in our uniform (and binary) presentation of convenience and utility in exchange for privacy: we simply controlled for it. Thus, in a manner consistent with contingency theory, the satisficing on constraints that users undertake as they consider privacy risk and trust exists on a wider and more nuanced scale than we have afforded in this study. This would also present an opportunity to examine this more closely in future research. Similarly, there are other covariates, such as experience or mobile self-efficacy, which are not included in this analysis, yet have been demonstrated to be salient in IT adoption decisions (Venkatesh et al. 2003). Future research should examine such factors.

A final, but by no means least important, concern is our willingness-to-pay (WTP) measure. Our results indicate that the WTP measure is not well understood by non-iPhone users, or, even among iPhone users – those who rarely, or never, pay for apps. We are not certain that pricing and value have stabilized in this market; this has possibly skewed and/or distorted our WTP measure resulting in the low variance explained (11.3 percent). Furthermore, as our treatment presented a hypothetical scenario, where users did not actually have to spend money, a vested basis for valuation is uncertain. However, we feel that this is a common problem with stated choice measurements. In remedy, future studies could present narrowing pricing bands based on a market review of existing apps.

There are also nascence concerns such that the phenomena we are studying are so new that the true causal relationships and underlying dynamics have not fully emerged. In this sense, we feel that the lifetime of LBS and their use is in an incipient phase; the findings of this research may change with extended LBS usage and, thus, necessitate follow-on research. In any case, this nascence does not belie an important fundamental detail regarding the diffusion of many other IT innovations: first impressions mean everything when there are many options to choose from. Therefore, if users cannot trust an app quickly, it may not matter anyway as alternatives will be found without much hassle. A related concern is that of extended app use such that this study does not explain how perceptions might change after extended use. Therefore, another direction for future research would compare the perceptions of existing iPhone users to non-users.

We also foresee other problems related to the four mobile applications selected for our study. This may contribute to selection bias in the same manner that our convenience sample would – is there a class or category of mobile app, relevant to the question of location privacy, which we didn't include that may have altered our results?

Another concern has to do with brand penetration and ubiquity. In many consumer cultures, there are some brands so strongly associated with a category type that their brand is mistaken for the classification itself. While this has both good and bad implications for a market, our concern arises from brand perceptions of the sort that equates a brand with expectations, standards and norms. Therefore, if National Geographic, Rand McNally, or Garmin produce mapping software, would I be inclined to ascribe quality and reliability to those apps based on my brand recognition? We believe more work is needed to understand these impacts in the mobile space and whether brand trust and loyalty will influence trust with respect to location privacy assurance. Moreover, we also wonder what role, if any users' perceptions of the quality and security of their provider's network have any bearing on trust?

Lastly, as discussed above, the potential to tie location data to a user's identification presents a compounded risk which was not examined in this study. If users understand this risk, it could have a significant impact on our results. Future research should examine 1) how well users understand this potential concern, and 2) how it impacts their adoption decisions in a model such as ours.

Conclusion

In summary, we find the new dimension of location privacy to be of primary concern to LBS adoption which is only increasing and evolving. The limited information provided by mobile app platforms (e.g. the app description, star rating, and network size available for each app in the Apple App Store) plays a significant role in determining users' intentions to disclose personal location data and adopt mobile apps. We hope this research will help to encourage the development of this stream and keep research at the forefront of practice and help not only to "observe and report," but also to "lead and guide" the development of LBS artifacts (Orlikowski et al. 2001).

References

AdMob "45 Million US Smartphone Users," in *AdMob Mobile Metrics*, http://metrics.admob.com, 2010.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), Dec, pp. 179-211.

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*, Englewood-Cliffs, NJ: Prentice Hall.

Angst, C.M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *Mis Quarterly* (33:2), June, pp. 339-370.

Ateniese, G., Curtmola, R., de Medeiros, B., and Davis, D. 2003."Medical Information Privacy Assurance: Cryptographic and System Aspects," in *Security in Communication Networks*, Springer Berlin, Berlin, pp. 199-218.

Awad, N.F., and Krishnan, M.S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled for Online Personalization," *MIS Quarterly*), March, pp. 13-28.

Barclay, D., Thompson, R., and Higgins, C. 1995. "The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use an Illustration," *Technology Studies* (2:2), pp. 285-309.

Bellavista, P., Kupper, A., and Helal, S. 2008. "Location-based services: Back to the future," *Ieee Pervasive Computing* (7:2), Apr-Jun, pp. 85-89.

Boudreau, M.C., Gefen, D., and Straub, D.W. 2001. "Validation in information systems research: A state-of-the-art assessment," *Mis Quarterly* (25:1), Mar, pp. 1-16.

Brandon, J. "Why You Need a Smartphone Application Strategy," in *CIO*, http://www.cio.com, 2010.

Burnham, T.A., Frels, J.K., and Mahajan, V. 2003. "Consumer switching costs: A typology, antecedents, and consequences," *Journal of the Academy of Marketing Science* (31:2), Spr, pp. 109-126.

Cameron, T.A., and James, M.D. 1987. "Estimating Willingness to Pay from Survey Data: An Alternative Pre-Test Market Evaluation Procedure," *Journal of Marketing Research* (24:4), Nov, pp. 389-395.

Chin, W.W. 1998. "Issues and opinion on structural equation modeling," *Mis Quarterly* (22:1), Mar, pp. VII-XVI.

Clarke, R. 2001. "Person location and person tracking: Technologies, risks and policy implications," *Information Technology & People* (14:2), pp. 206-231.

Colquitt, J.A., Conlon, D.E., Wesson, M.J., Porter, C.O.L.H., and Yee Ng, K. 2001. "Justice at the Millennium: A Meta-Analytic Review of 25 Years of Organizational Justice Research," *Journal of Applied Psychology* (86:3), pp. 425-445.

Culnan, M.J. 1993. "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *Mis Quarterly* (17:3), Sep, pp. 341-361.

Culnan, M.J., and Armstrong, P.K. 1999. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science* (10:1), Jan-Feb, pp. 104-115.

Damianides, M. 2004. "Sarbanes–Oxley and it Governance: New Guidance on it Control and Compliance," *EDPACS: The EDP Audit, Control, and Security Newsletter* (31:10), April, pp. 1-14.

Davis, F.D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *Mis Quarterly* (13:3), Sep, pp. 319-340.

DeLone, W.H., and McLean, E.R. 2003. "The DeLone and McLean model of information systems success: a ten-year update," *Journal of Management Information Systems* (19:4), Spr, pp. 9-30.

DeSmith, M.J., Goodchild, M.F., and Longley, P. 2007. *Geospatial Analysis: A Comprehensive Guide to Principles, Techniques and Software Tools*, Leicester: Matador.

Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for E-commerce transactions," *Information Systems Research* (17:1), Mar, pp. 61-80.

Duan, W., Gu, B., and Whinston, A.B. 2009. "Informational Cascades and Software Adoption on the Internet: An Empirical Investigation," *Mis Quarterly* (33:1), Mar, pp. 23-48.

Duh, R.-R., Sunder, S., and Jamal, K. 2002. "Control and Assurance in E-Commerce: Privacy, Integrity, and Security at eBay," *Taiwan Accounting Review* (3:1), October, pp. 1-27.

Farrell, J., Klemperer, P., Armstrong, M., and Porter, R. 2007."Coordination and Lock-In: Competition with Switching Costs and Network Effects," in *Handbook of Industrial Organization*, Elsevier, pp. 1967-2072.

Featherman, M.S., and Pavlou, P.A. 2003. "Predicting e-services adoption: a perceived risk facets perspective," *International Journal of Human-Computer Studies* (59:4), Oct, pp. 451-474.

Fornell, C., and Bookstein, F.L. 1982. "Two structural equation models: LISREL and PLS applied to consumer exit-voice theory," *Journal of Marketing Research* (19:4), pp. 440-452.

Fornell, C., and Larcker, D.F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.

Gefen, D. 2000. "E-commerce: the role of familiarity and trust," *Omega-International Journal of Management Science* (28:6), Dec, pp. 725-737.

Gefen, D., Karahanna, E., and Straub, D.W. 2003. "Trust and TAM in Online Shopping: An Integrated Model," *Mis Quarterly* (27:1), pp. 51-90.

Gefen, D., Streeter, L.A., and Boudreau, M.-C. 2000. "Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice," *Communications of the AIS* (7:7), pp. 1-78.

Gigaom "The Apple App Store Economy," in, gigaom.com, 2010.

GovTech "Survey Raises Consumer Online Privacy Awareness," in *Governement Technology Magazine*, Government Technology, 2009.

Haag, S., and Cummings, M. 2009. *Information Systems Essentials*: McGraw-Hill, Inc., p. 464.

Homburg, C., Koschate, N., and Hoyer, W.D. 2005. "Do satisfied customers really pay more? A study of the relationship between customer satisfaction and willingness to pay," *Journal of Marketing* (69:2), Apr, pp. 84-96.

Hu, X.R., Lin, Z.X., Whinston, A.B., and Zhang, H. 2004. "Hope or hype: On the viability of escrow services as trusted third parties in online auction environments," *Information Systems Research* (15:3), Sep, pp. 236-249.

Hui, K.L., Teo, H.H., and Lee, S.Y.T. 2007. "The value of privacy assurance: An exploratory field experiment," *Mis Quarterly* (31:1), Mar, pp. 19-33.

Katz, M.L., and Shapiro, C. 1985. "Network Externalities, Competition, and Compatibility," *American Economic Review* (75:3), pp. 424-440.

Kauffman, R.J., McAndrews, J., and Wang, Y.M. 2000. "Opening the "black box" of network externalities in network adoption," *Information Systems Research* (11:1), Mar, pp. 61-82.

Keith, M.J., Raghu, T.S., and Sinha, R. 2010."Switching Costs, Satisfaction, Loyalty and Willingness to Pay for Office Productivity Software," Proceedings of the 44th Hawaiian International Conference on System Sciences, Koloa, HI, pp. 1-9.

Kincaid, J. "comScore: Android Market Share Continues to Gain on the iPhone," in *TechCrunch*, TechCrunch, 2010.

Komiak, S.Y.X., and Benbasat, I. 2006. "The effects of personalization and familiarity on trust and adoption of recommendation agents," *Mis Quarterly* (30:4), Dec, pp. 941-960.

Krishna, A. 1991. "Effect of Dealing Patterns on Consumer Perceptions of Deal Frequency and Willingness to Pay," *Journal of Marketing Research* (28:4), Nov, pp. 441-451.

Laufer, R.S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22-42.

Malhotra, N.K., Sung, K.S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the scale and a Causal Model," *Information Systems Research* (14:4), December, pp. 336-355.

Mason, R.O. 1986. "Four Ethical Issues of the Information Age," *Mis Quarterly*), March, pp. 5-12.

McFadden, D. 1986. "The Choice Theory Approach to Market Research," *Marketing Science* (5:4), January 1, 1986, pp. 275-297.

McKnight, D.H., Choudhury, V., and Kacmar, C. 2002. "Developing and validating trust measures for e-commerce: An integrative typology," *Information Systems Research* (13:3), Sep, pp. 334-359.

Orlikowski, W., and Iacono, C.S. 2001. "Desperately Seeking the "IT" in IT Research - A Call to Theorizing the IT Artifact"," *Information Systems Research* (12:2), June, pp. 121-134.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., and Podsakoff, N.P. 2003. "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), Oct, pp. 879-903.

Raghu, T.S., Sinha, R., Vinze, A., and Burton, O. 2009. "Willingness to Pay in an Open Source Software Environment," *Information Systems Research* (20:2), Jun, pp. 218-236.

Rainie, L. "Internet, broadband, and cell phone statistics," Pew Internet & American Life Project.

Ramnath, C.K., and Sin, R.G. 2005. "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6:2-3), April, pp. 181-202.

Rogers, E.M. 2003. *Diffusion of Innovations*, New York: Free Press.

Saadi, L., Langheinrich, M., and Röcker, C. 2005. "Privacy and Trust Issues with Invisible Computers," *Communications of the Acm* (48:3), March, pp. 59-60.

Samuelson, P. "Social Costs of Incoherent Privacy Policies," in *An Almaden Institute Symposium on Privacy*, IBM Almaden Privacy Institute, San Jose, California, USA, 2003.

Samuelson, P. "Information Law and Policy Video Lectures," in, UC California, Berkeley, Berkeley, CA, 2008.

Seddon, P.B. 1997. "A respecification and extension of the DeLone and McLean model of IS success," *Information Systems Research* (8:3), Sep, pp. 240-253.

Seriot, N. 2010."iPhone Privacy," Black Hat DC 2010, Black Hat, Arlington, Virginia, p. 30.

Sheng, H., Nah, F.F.H., and Siau, K. 2008. "An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns," *Journal of the Association for Information Systems* (9:6), pp. 344-377.

Simon, H.A. 1982. *Models of Bounded Rationality*, Cambridge, MA: MIT Press.

Smith, H.J., Milberg, S.J., and Burke, S.J. 1996. "Information Privacy: Measuring Individual's Concerns about Organizational Practices," *Mis Quarterly*), June, pp. 167-196.

Stone, E.F., Gardner, D.G., Geuetal, H.G., and McClure, S. 1983. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology*), pp. 459-468.

Straub, D.W. 1989. "Validating Instruments in MIS Research," *Mis Quarterly* (13:2), Jun, pp. 147-169.

Straub, D.W., and Collins, R.W. 1990. "Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy," *Mis Quarterly*), June, pp. 143-156.

Tabachnick, B.G., and Fidell, L.S. 2000. *Using Multivariate Statistics*, Upper Saddle River, NJ: Allyn & Bacon.

Vance, A., Elie-Dit-Cosaque, C., and Straub, D.W. 2008. "Examining trust in information technology artifacts: The effects of system quality and culture," *Journal of Management Information Systems* (24:4), Spr, pp. 73-100.

Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. 2003. "User acceptance of information technology: Toward a unified view," *Mis Quarterly* (27:3), Sep, pp. 425-478.

Williamson, O.E. 1981. "The Economics of the Organization: The Transaction Cost Approach," *American Journal of Sociology* (87:3), pp. 548-577.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," *Proceedings of the International Conference on Information Systems*), December 14-17.

Xu, H., Teo, H.H., Tan, B.C.Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), Win, pp. 135-173.